(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
13 octobre 2005 (13.10.2005)

PCT

(10) Numéro de publication internationale
WO 2005/096135 A2

(51) Classification internationale des brevets[7] : G06F 7/52

(21) Numéro de la demande internationale :
PCT/FR2005/000443

(22) Date de dépôt international :
24 février 2005 (24.02.2005)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0402146 2 mars 2004 (02.03.2004) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **GIRAULT, Marc** [FR/FR]; 4, rue Viviane, F-14000 Caen (FR). **LEFRANC, David** [FR/FR]; Résidence Stéphanolyse, 7, rue des Tilleuls, F-14000 Caen (FR).

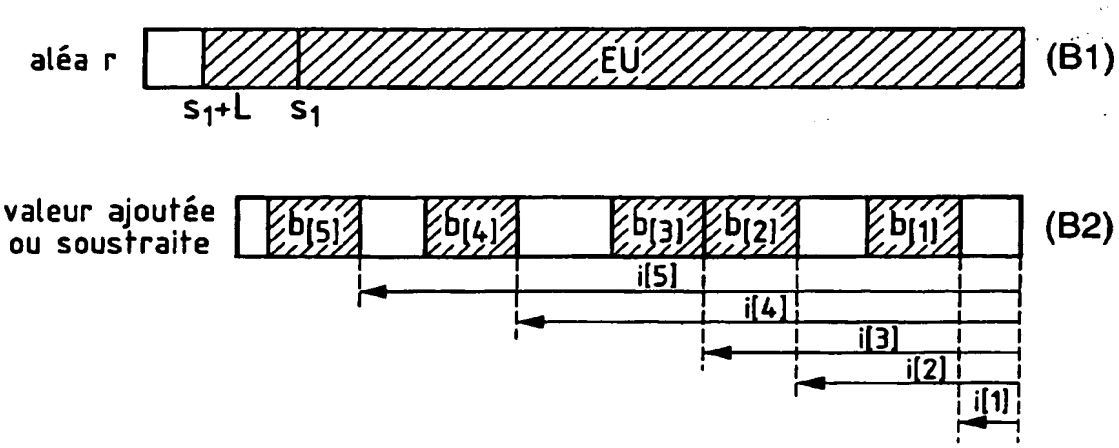
(74) Mandataires : **LOISEL, Bertrand** etc.; Cabinet Plasseraud, 65/67, rue de la Victoire, F-75440 Paris Cedex 09 (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM,

[Suite sur la page suivante]

(54) Title: METHOD AND DEVICE FOR PERFORMING A CRYPTOGRAPHIC OPERATION

(54) Titre : PROCEDE ET DISPOSITIF POUR ACCOMPLIR UNE OPERATION CRYPTOGRAPHIQUE



(B1) ... RANDOM
(B2) ... INCREMENT OR SUBTRACTED VALUE

(57) Abstract: The inventive method for performing a cryptographic operation by a device controlled by the security application executed outside thereof consists in producing a cryptographic value (y) in the device by a calculation comprising at least one multiplication between first and second factors containing a security key (s) associated with the device and a challenge number (c) provided by the security application. The first multiplication factor comprises a determined number of bits (L) in a binary representation. The second factor is constrained in such a way that it comprises; in a binary representation, several bits at 1 with a sequence of at least L-1 bits at 0 between each pair of consecutive bits to 1 and the multiplication is carried out by assembling the binary versions of the first factor shifted according to positions of the bits at 1 of the second factor, respectively.

[Suite sur la page suivante]

WO 2005/096135 A2

TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **États désignés** *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclaration en vertu de la règle 4.17 :

— *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

Publiée :

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : Pour accomplir une opération cryptographique dans un dispositif sous le contrôle d'une application de sécurité exécutée en dehors du dispositif, on produit une valeur cryptographique (y) dans le dispositif, par un calcul comprenant au moins une multiplication entre des premier et second facteurs incluant une clé secrète (s) associée au dispositif et un nombre (C) dit challenge fourni par l'application de sécurité. Le premier facteur de la multiplication comprend un nombre de bits déterminé L en représentation binaire. On contraint le second facteur pour qu'il comprenne, en représentation binaire, plusieurs bits à (1) avec, entre chaque paire de bits à (1) consécutifs, une séquence d'au moins L-1 bits à (0), et en ce que la multiplication est réalisée en assemblant des versions binaires du premier facteur respectivement décalées conformément aux positions des bits à (1) du second facteur.